SELECTED CASE HISTORIES
NERC CIP STANDARDS V. NIST 800-53

According to a NIST-commissioned technical review, NERC Reliability Standards are both "inadequate for protecting critical national infrastructure," and "inadequate for all electric energy systems when the impact of regional and national power outages is considered."[1] But what happens when the NERC and NIST standards are applied to actual incidents?

SQL Slammer Worm, January 25, 2003

- Issue: The "SQL Slammer Worm" affects the ability of the telecommunications relay to communicate to the substations. SCADA traffic is completely blocked, *leading to loss of communications between the control center and substations.*
- Problem: The NERC CIP Standard excludes telecommunications equipment from being considered "critical cyber assets." NIST SP800-53 does not have the same exclusion.

Tempe, Arizona, June 29, 2007

- Issue: An outage occurred in the Tempe, Arizona area caused by the unexplained activation of the distribution load shedding program in the energy management system (EMS). Most of the automation in the electric transmission and distribution systems are from distribution systems. Distribution systems can be directly connected to transmission systems and distribution system failures can be precursors to cascading outages.
- Problem: The NERC CIP Standard excludes distribution systems from being considered "critical cyber assets." NIST SP800-53 does not have the same exclusion.

Australian Sewage Spill, April 23, 2000

- Issue: Vitek Boden worked for an Australian firm that installed SCADA radio-controlled sewage equipment. He packed his car with stolen radio equipment attached to a computer. He drove around issuing radio commands to the sewage equipment that resulted in sewage spills. This is the first widely known example of someone maliciously breaking into a control system.
- Problem: The NERC CIP Standard excludes telecommunications and non-routable protocols and does not explicitly address wireless systems in the definition of "critical cyber assets." NIST SP800-53 does not have these exclusions and directly addresses wireless communications.

Browns Ferry Nuclear Plant, August 19, 2006

- Issue: Operators at Browns Ferry, Unit 3, manually scrammed (shut down) the unit following a loss of both the 3A and 3B reactor recirculation pumps. The loss was caused from "excessive traffic" on the connected plant Integrated Control System (ICS) network. Nuclear plants represent approximately 20% of the U.S. electric generation. Shutdown of nuclear facilities would have a significant impact on the reliability of the bulk electric grid. The NRC is responsible for the "safe shutdown," but not the "continued operation" of nuclear plants to provide grid reliability.
- Problem: The NERC CIP Standard excludes nuclear power facilities. NIST SP800-53 does not have exclusions for nuclear plants.

[1] Marshall D. Abrams, "Addressing Industrial Control Systems in NIST Special Publication 800-53," MITRE Technical Report (March 2007), p. 2-20.